UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/731,029	12/10/2003	Frederic Gariador	ALC 3104	5164

7590 09/06/2007

KRAMER & AMADO, P.C.
Suite 240
1725 Duke Street
Alexandria, VA 22314

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
09/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/731,029	GARIADOR ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed June 22, 2007, have been fully considered but they are not persuasive.

2. Claims 1-20 are pending and have been examined.

Response to Amendment

3. The objections to the specification are withdrawn.

4. The objection to claim 19 is withdrawn.

5. The rejection of claims 15 and 20 under 35 U.S.C. 112, first paragraph, is withdrawn.

6. Regarding Applicant's argument that Thomsen does not teach storing "a copy" or "comparing the copy to the frame received", Examiner respectfully points to Thomsen's claim language, where "In a network comprising a number of segments, said number being at least one, each of said segments comprising at least one node, and at least one device with a unique identifier coupled into said network via said node, a method of monitoring said network, said method comprising: monitoring a plurality of data packets on said network; detecting one packet of said data packets having an origination address identical to said unique identifier; comparing said one packet to a record of packets sent by said device; and upon determining that said one packet did not originate at said device, initiating an action wherein said action is selected from the group consisting of: suspending access to said segment; initiating prophylaxis; and initiating correction (claim 1)." This language, clearly teaches and suggest, storing information about something sent (whether an identifier or the whole packet/frame sent

is irrelevant), comparing something received to something sent, to determine if it was sent by the receiver node, and taking some corrective measure/action. **Applicant's arguments are not persuasive.**

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomsen (US Patent 6,745,333).

Regarding claim 1, Thomsen teaches

- A method for detecting impersonation based attacks at a wireless node of a wireless communication network, comprising the steps of: **(abstract)**
- a) operatively connecting the wireless node with an intrusion detection module and providing the intrusion detection module with INFORMATION SENT of original data frames transmitted by the wireless node over a wireless interface **(col. 12, lines 33-67, claim 1)**;
- b) detecting at the intrusion detection module incoming data frames received over the wireless interface **(col. 12, lines 50-67, col. 13, lines 1-28)**; and

- c) comparing at the intrusion detection module the information in the INFORMATION SENT with the information in the incoming data frames **(claim 1)**; and
- d) recognizing an impersonating attack when the intrusion detection module determines that the information in the INFORMATION SENT differs from the information in the incoming data frames **(col. 10, lines 50-67, col. 11, lines 1-33)**.

Thomsen does not expressly disclose that the information sent is a COPY of the packet/frame sent, but teaches to compare information sent with information received/ captured to make an informed decision as to the authenticity of network traffic. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store some or all information pertaining a packet / frame sent for later usage to determine whether traffic received is bona fide as long as the information stored helped in making such determination. One of ordinary skill in the art would have been motivated to perform such a modification since Thomsen suggest comparing other unique features of information sent/received (col. 20, lines 15-55, col. 21, lines 35-67, col. 22, lines 1-22, claim 1).

Regarding claim 10, Thomsen teaches

- an impersonation detection system for a wireless node of a wireless communication network, the node for transmitting original data frames over a wireless interface **(abstract)** comprising:

- an intrusion detection module for correlating the original data frames with incoming data frames received over the air interface **(col. 12, lines 33-67, claim 1)**; and
- connection means between the wireless node and the intrusion detection module for providing the intrusion detection module with INFORMATION SENT of the original data frames **(col. 12, lines 50-67, col. 13, lines 1-28, claim 1)**.

Thomsen does not expressly disclose that the information sent is a COPY of the packet/frame sent, but teaches to compare information sent with information received/ captured to make an informed decision as to the authenticity of network traffic. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store some or all information pertaining a packet / frame sent for later usage to determine whether traffic received is bona fide as long as the information stored helped in making such determination. One of ordinary skill in the art would have been motivated to perform such a modification since Thomsen suggest comparing other unique features of information sent/received (col. 20, lines 15-55, col. 21, lines 35-67, col. 22, lines 1-22, claim 1).

Regarding claim 17, Thomsen teaches

- wireless node for a wireless network comprising **(abstract)**:
- means for transmitting outgoing data frames over a wireless interface **(col. 12, lines 33-67)**;

- an intrusion detection module for correlating the outgoing data frames with incoming data frames received from the air interface **(col. 12, lines 33-67, col. 13, lines 1-28, claim 1)**; and
- a secure link between the wireless node and the intrusion detection module for providing the intrusion detection module with INFORMATION of the outgoing data frames **(col. 10, lines 50-67, col. 11, lines 1-33, col. 12, lines 50-67, col. 13, lines 1-28, claim 1)**.

Thomsen does not expressly disclose that the information sent is a COPY of the packet/frame sent, but teaches to compare information sent with information received/ captured to make an informed decision as to the authenticity of network traffic. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store some or all information pertaining a packet / frame sent for later usage to determine whether traffic received is bona fide as long as the information stored helped in making such determination. One of ordinary skill in the art would have been motivated to perform such a modification since Thomsen suggest comparing other unique features of information sent/received (col. 20, lines 15-55, col. 21, lines 35-67, col. 22, lines 1-22, claim 1).

Regarding claim 2, Thomsen teaches wherein step a) comprises transmitting the copy over a secure link established between the wireless node and the intrusion detection module **(col. 1, lines 50-67)**.

Regarding claim 3, Thomsen teaches wherein the copy comprises only management frames **(col. 11, lines 50-67, col. 12, lines 1-18)**.

Regarding claim 4, Thomsen teaches wherein the copy includes a summary of the outgoing data frames **(col. 12, lines 33-67)**.

Regarding claim 5, Thomsen teaches wherein the summary of the outgoing data frames comprises frames that allow statistical comparisons **(col. 12, lines 50-67)**.

Regarding claim 6, Thomsen teaches wherein the summary comprises the number of the outgoing data frames transmitted over a time interval **(col. 12, lines 33-67)**.

Regarding claim 7, Thomsen teaches wherein the summary comprises the types of the original data frames **(col. 11, lines 50-67, col. 12, lines 33-67)**.

Regarding claim 8, Thomsen teaches wherein step b) comprises monitoring all wireless channels allocated to the wireless node and extracting the incoming data frames received over all the wireless channels allocated to the wireless node **(col. 15, lines 30-67)**.

Regarding claim 9, Thomsen teaches wherein step d) comprises: correlating the original data frames with the incoming data frames for detecting an inconsistency between the frames; and upon detection of the inconsistency, further processing the incoming data frames for qualifying the impersonating attack **(col. 10, lines 50-67, col. 11, lines 1-33)**.

Regarding claim 11, Thomsen teaches wherein the intrusion detection module comprises: a first receiving unit for receiving the copy; an antenna for capturing the incoming traffic received on all transmission channels allocated to the wireless node; a second receiving unit for detecting the incoming data frames from the incoming traffic;

and a data processing unit for correlating the copy with the incoming data frames and generating a impersonation detection signal **(col. 9, lines 1-15, col. 12, lines 50-67, col. 13, lines 1-28)**.

Regarding claim 12, Thomsen teaches wherein the intrusion detection module further comprises means for qualifying an intrusion attack based on the impersonation detected signal **(col. 10, lines 50-67, col. 11, lines 1-33)**.

Regarding claim 13, Thomsen teaches wherein the connection means comprises, when the intrusion detection module resides away from the wireless node: a transmitting unit on the wireless node, for transmitting the copy to the intrusion detection module; and a secure link for connecting the wireless node with the intrusion detection module **(col. 15, lines 30-67)**.

Regarding claim 14, Thomsen teaches wherein the secure link operates according to a communication protocol **(col. 1, lines 50-67)**.

Regarding claim 16, Thomsen teaches wherein the secure link is established as inter-processes communication, when the intrusion detection module is integrated within the wireless node **(col. 8, lines 18-50)**.

Regarding claim 18, Thomsen teaches wherein the intrusion detection module comprises: a first receiving unit for receiving the copy of the outgoing data frames; an antenna for capturing the incoming traffic carried on all transmission channels allocated to the wireless node; a second receiving unit for detecting the incoming data frames from the incoming traffic; and a data processing unit for correlating the copy of the

outgoing data frames with the incoming data frames and generating an impersonation detected signal **(col. 10, lines 50-67, col. 11, lines 1-33)**.

Regarding claim 19, Thomsen teaches wherein the intrusion detection module further comprises means for qualifying an intrusion attack based on the impersonation detected signal **(col. 10, lines 50-67, col. 11, lines 1-33)**.

Regarding claims 15 and 20, Thomsen teaches wherein the wireless network operates according to any wireless network technology **(abstract)**.

Conclusion

9. **Examiner's Note:** Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

11. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

12. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8, 31, 07